CLAIMS

What is claimed is:

1. A method for performing secure ephemeral communication comprising:

receiving at a first node a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

securely communicating said doubly wrapped value to said second node;

obtaining a second decryption key having a predetermined expiration time at a second node;

decrypting said doubly wrapped value using said second decryption key to produce said singly wrapped value if said second decryption key has not expired; and

securely communicating said singly wrapped value to a third node.

2. The method of claim 1 further including the step of generating in a fourth node said triply wrapped value and communicating said triply wrapped value for receipt by said first node.



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

3. The method of claim 1 wherein said first node and said third node are the same node.

4. The method of claim 1 further including the step of decrypting said singly wrapped value to obtain said value using said first decryption key.

5. The method of claim 1 wherein said first encryption and decryption keys comprise a first public and private key pair.

6. The method of claim 1 wherein said second encryption and decryption keys comprise a second public and private key pair.

7. The method of claim 1 wherein said third encryption and decryption keys comprise a third public and private key pair.

8. The method of claim 1 wherein said step of securely communicating said singly wrapped value to said third node comprises the steps of securely communicating said singly wrapped value from said second node to said first node and securely communicating said singly wrapped value from said first node to said third node.

9. The method of claim 1 further including the steps of:

receiving at said first node an identifier associated with said second node; and

forwarding said doubly wrapped value to said second node at an address associated with said identifier.

10. The method of claim 9 wherein said identifier comprises a uniform resource locator associated with said second node.



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

11. The method of claim 1 wherein said step of securely communicating said doubly wrapped value to said second node comprises the steps of:

encrypting said doubly wrapped value with a fourth encryption key to form an encrypted doubly wrapped value, wherein said fourth encryption key has a corresponding fourth decryption key;

encrypting said fourth decryption key with said second encryption key;

communicating said encrypted fourth decryption key and said doubly wrapped value from said first node to said second node;

decrypting said encrypted fourth decryption key to obtain said fourth decryption key using said second decryption key in the event said second decryption key has not expired;

decrypting said encrypted doubly wrapped value using said fourth decryption key to obtain said doubly wrapped value.

12. The method of claim 11 wherein said fourth encryption and decryption keys comprise symmetric keys.

13. The method of claim 11 further including the steps of encrypting said fourth encryption key with said second encryption key and communicating said encrypted fourth encryption key to said second node; and

wherein said step of securely communicating said singly wrapped value to a third node comprises the steps of:

decrypting said encrypted fourth encryption key using said second decryption key to obtain said fourth encryption key, in the event said second decryption key has not expired;



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

encrypting said doubly wrapped value with said fourth encryption key to obtain a securely wrapped value;

communicating said securely wrapped value from said second node to said third node; and

decrypting said securely wrapped value using said fourth decryption key to obtain said doubly wrapped value.

14. The method of claim 13 wherein said fourth encryption and decryption keys comprise symmetric keys.

15. The method of claim 2 wherein said value comprises a first secret key and said method further includes the steps of:

encrypting information with said first secret key to form an encrypted information value;

communicating said encrypted information value from said fourth node to said third node;

decrypting said singly wrapped value at said third node using said third decryption key to obtain said first secret key; and

decrypting said encrypted information value at said third node using said first secret key.

16. The method of claim 15 further including the step of deleting said first secret key at said second node subsequent to decrypting said encrypted information value.

17. The method of claim 1 further including the step of receiving at said second node a key identifier associated with said second decryption key and said obtaining step comprises the step of using said key identifier to select said second



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

decryption key from a plurality of decryption keys accessible by said second node.

18. A method for performing secure ephemeral communication comprising:

receiving at a first node a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form said doubly wrapped value;

receiving at said first node an integrity verification key securely associated with said doubly wrapped value;

communicating from a second node to said first node proof that said second node is an authorized decryption agent for said value;

obtaining at said first node a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value in the event said second decryption key has not expired;

verifying said proof at first node using said integrity verification key to ascertain whether said second node is an authorized decryption agent for said value; and

in response to verification that said second node is an authorized decryption agent for said value, securely communicating said singly wrapped value to said second node.

19. The method of claim 18 further including the step of decrypting said singly wrapped value to obtain said value using a first decryption key associated with said first encryption key and accessible to said second node.



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

20. The method of claim 18 wherein said first encryption and decryption keys comprise first public and private keys of a public-private key pair associated with said second node.

21. The method of claim 18 wherein said second encryption and decryption keys comprise second public and private keys of a second public-private key pair associated with said first node.

22. The method of claim 18 wherein said integrity verification key comprises said first public key associated with said second node and said securely associating step includes the step of encrypting said singly wrapped value and said first public key with said second encryption key, said step of communicating said proof that said second node is an authorized decryption agent for said value includes the step of generating by said second node a digital signature using said second node private key, and said verifying step includes the step of verifying said digital signature at said first node using said second node public key.

23. The method of claim 18 wherein said step of communicating said proof that said second node is an authorized decryption agent for said value includes the step of securely communicating from said second node to the first node said proof that said second node is an authorized decryption agent for said value.

24. The method of claim 18 wherein said step of securely communicating said singly wrapped value from said first node to said second node includes the steps of:

encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein said third



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

encryption key has a corresponding third decryption key accessible to said second node;

communicating said encrypted singly wrapped value from said first node to said second node; and

decrypting said encrypted singly wrapped value using said first decryption key to obtain said value.

25. The method of claim 23 wherein said third encryption and decryption keys comprise a first symmetric key pair.

26. The method of claim 19 wherein said value comprises a secret key and said method further includes the steps of:

receiving at said second node an encrypted information payload comprising an information payload encrypted with said secret key; and

decrypting said encrypted information payload at said second node using said secret key.

27. A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with s second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

program code within said first node memory for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

program code within said first node memory for securely communicating said doubly wrapped value to said second node;

program code for obtaining a second decryption key having a predetermined expiration time at said second node, wherein said second decryption key is associated with said second encryption key;

program code within said second node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if said second decryption key has not expired; and

program code within said second node memory for securely communicating said singly wrapped value to a third node following decryption of said doubly wrapped value.

28. The system of claim 27 further including program code within said third node memory for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

29. The system of claim 27 wherein said first and third nodes are the same node, said first and third encryption keys are the same and said first and third decryption keys are the same.

30. A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value;

program code within said first node memory for receiving an integrity verification key securely associated with said doubly wrapped value;

program code within said second node for communicating from said second node to said first node proof that said second node is an authorized decryption agent for said value;

program code within said first node for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

program code within said first node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value in the event said second decryption key has not expired;

program code within said first node memory for verifying said proof at first node using said integrity verification key to ascertain whether said second node is an authorized decryption agent for said value; and

program code within said first node memory for securely communicating said singly wrapped value to said second node in response to verification that said second node is an authorized decryption agent for said value.

31. The system of claim 30 further including program code within said second node memory for decrypting said singly wrapped value



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

using a first decryption key associated with said first encryption key.

32. A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means associated with said first node for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with s second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

means associated with said first node for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

means associated with said first node memory for securely communicating said doubly wrapped value to said second node;

means associated with said second node for obtaining a second decryption key having a predetermined expiration time, wherein said second decryption key is associated with said second encryption key;

means associated with said second node for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if said second decryption key has not expired; and

means associated with said second node memory for securely communicating said singly wrapped value to a third node following decryption of said doubly wrapped value.



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

33. The system of claim 32 further including means associated with said third node for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

34. The system of claim 32 wherein said first and third nodes are the same node.

35. A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means associated with said first node for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value;

means associated with said first node for receiving an integrity verification key securely associated with said doubly wrapped value;

means associated with said second node for communicating from said second node to said first node proof that said second node is an authorized decryption agent for said value;

means associated with said first node for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

means associated with said first node for decrypting said doubly wrapped value using said second decryption key to obtain



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

said singly wrapped value in the event said second decryption key has not expired;

means associated with said first node for verifying said proof at first node using said integrity verification key to ascertain whether said second node is an authorized decryption agent for said value; and

means associated with said first node for securely communicating said singly wrapped value to said second node in response to verification that said second node is an authorized decryption agent for said value.

36. The system of claim 35 further including means for decrypting said singly wrapped value using a first decryption key accessible to said second node and associated with said first encryption key.



ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313